ASSOCIATED FORMS IN THE GENERAL THEORY OF MODULAR COVARIANTS.

By Olive C. Hazlett.

1. Historical Background.—In any theory of covariants, it is of prime importance to ascertain whether or not all covariants of the set are expressible as functions of the covariants belonging to a finite subset. We may attack this fundamental problem from either one of two different points of view: either we may endeavor to express all covariants of the set as rational integral functions of the covariants of a finite subset, or we may content ourselves with the problem of finding rational relations (syzygies) connecting the covariants. The first leads to the finiteness theorem; the second, to the theory of associated forms. Whichever problem we attack, there emerge two entirely different theories, according as the coefficients of the transformations of the group are marks of a field of characteristic zero or marks of a field of characteristic $p \neq 0$.

In the theory of algebraic covariants of a system of forms under a group of transformations having the coefficients in a field of characteristic zero, both problems have been successfully attacked. The most important names to be associated with the first problem are, Gordan, Mertens, and Hilbert;* with the second problem, we associate the names of Boole, Hermite and Clebsch.†

In the theory of algebraic covariants of a system of forms under a group of linear transformations whose coefficients are marks of a field of character $p \neq 0$, comparatively little has as yet been accomplished on either of these problems. It must be remembered that, in the case of a finite field, there present themselves two distinct kinds of algebraic covariants in contrast to the single kind of algebraic covariant that arises when the field is of characteristic zero. For, in the latter field, if a function be unaltered in form, it is unaltered in value and conversely. Whereas, in a finite field, if a function be unaltered in form it is unaltered in value, but the converse

* Gordan, numerous articles in the journals (for references, see the German encyclopedia, IB2, § 6) especially *Journal für Mathematik*, Vol. 69 (1868), pp. 323–354, *Mathematische Annalen*, Vol. 2 (1870), pp. 227–280. Also his "Invariantentheorie," Vol. 2, pp. 231–236; Mertens, *Journal für Mathematik*, Vol. 100 (1887), pp. 223–230; Hilbert, *Mathematische Annalen*, Vol. 36 (1890), pp.473.

† Boole, *Cambridge Mathematical Journal*, Vol. 3 (1841), pp. 1–20, 106–119; Hermite, *Journal für Mathematik*, Vol. 52 (1856), pp. 1–38; Clebsch, *Mathematische Annalen*, Vol. 3 (1871), pp. 265–267, and "Theorie der binären algebraischen Formen" (1872), p. 410.

is not true in general, in view of Galois' generalization of Fermat's theorem.* Accordingly, then, we distinguish two kinds of algebraic covariants of a system of forms under a group of linear transformations with coefficients in the Galois field $GF[p^n]$—formal (modular) covariants and modular covariants, according as the coefficients of the original form are regarded as independent variables or as marks of the field.

The first to consider formal invariants was Hurwitz,† who found that they arose naturally in an inquiry into the number of roots of the congruence $a_r x^r + a_{r-1} x^{r-1} + \cdots + a_1 x_1 + a_0 \equiv 0 \pmod{p}$. He proved the finiteness theorem for formal invariants for the special case where the order of the group G is not divisible by p‡. This case is of only minor importance; for the total linear group of transformations whose coefficients are in the field $GF[p^n]$ is of order $p^n(p^n - 1)(p^{2n} - 1)$ which is congruent to zero modulo p. Four years later, Dickson introduced the notion of modular invariants§ and published an elegant theory of modular invariants in which he proved that there is only a finite number of modular invariants of any system of forms under any group G of linear transformations.|| Four years later, Dickson proved that the set of all modular covariants of any system of forms possesses the finiteness property, i.e., they are all expressible as polynomials in the covariants belonging to a finite subset.** In 1914, one of Dickson's students extended this theorem to the modular invariants of a system of forms and a number of cogredient binary points.†† Up to the present, the finiteness theorem has been proved for formal covariants only in very special cases—these are due to Professor Glenn.‡‡ As Hurwitz pointed out, this is a most difficult problem, for none of the methods that obtain in the classical theory of algebraic covariants will apply here.

* If a is a mark of a finite field F of order p^n, then $a^{p^n} \equiv a$ in the field. In case $n = 1$ the marks of the field are the classes of residues of integers reduced modulo p, and Galois' theorem reduces to Fermat's theorem.

† "Ueber höhere Congruenzen," *Archiv der Mathematik und Physik*, series 3, Vol. 5 (1903), pp. 17–27.

‡ Loc. cit., p. 25.

§ "Invariants of binary forms under modular transformations," *Transactions of the American Mathematical Society*, Vol. 8 (1907), pp. 205–232.

|| "General Theory of Modular Invariants," *Transactions of the American Mathematical Society*, Vol. 10 (1909), pp. 123–158. This is the basic paper on modular invariants.

** "Proof of the Finiteness of Modular Covariants," *Transactions of the American Mathematical Society*, Vol. 14 (1913), pp. 299–310.

†† F. B. Wiley, "Proof of the Finiteness of the Modular Covariants of a System of Binary Forms and Cogredient Points," *Transactions of the American Mathematical Society*, Vol. 15 (1914), pp. 431–438.

‡‡ "A Fundamental System of Formal Covariants Modulo 2 of the Binary Cubic," *Transactions of the American Mathematical Society*, Vol. 19 (1918), pp. 109–118; "Modular Concomitant Scales, with a Fundamental System of Formal Covariants, Modulo 3, of the Binary Quadratic," *Transactions*, Vol. 20 (1919), pp. 154–168.

Hence, since this problem is so intractable, it may be of interest to consider the related problem of syzygies. The present paper extends the method and results of Hermite's fundamental memoir on associated forms for ordinary algebraic covariants to modular covariants, both formal and otherwise. The main theorem proves that, if $f = a_0x_1 + a_1x^{m-1} + \cdots$ is a binary form of order not divisible by p, then any modular covariant of f for the Galois Field $GF[p^n]$ of order p^n is expressible (aside from a power of f) as a polynomial in the universal covariants Q and L, where the coefficients of the terms in Q are polynomials in the forms associated with f. We also prove an analogous theorem for formal covariants. From the first of these we prove the rather striking corollary that, aside from a power of f, every modular covariant is congruent to an ordinary algebraic covariant of f whenever the variables x and y are in the field. Similarly we prove that, aside from a power of a_0, every modular invariant is congruent to an ordinary algebraic invariant of f. Another corollary gives a neat method of constructing a modular covariant having a given leader, provided the leader has a_0 as a factor. The main theorem, together with its corollaries, is verified for the binary quadratic, modulo 3.

2. Hermite's Two Propositions.—In a fundamental memoir* already mentioned, Hermite proves the following

FIRST PROPOSITION. *Let g and h be any two algebraic covariants of the form $f(x, y) = a_0x^m + a_1x^{m-1}y + \cdots + a_my^m$ of indices s and t respectively, and let us set*

$$g\left(a_0, a_1, a_2, \cdots;\ xX - \frac{\partial h}{\partial y}Y,\ yX + \frac{\partial h}{\partial x}Y\right) \tag{1}$$

$$= \theta(a_0, a_1, a_2, \cdots;\ x, y;\ X, Y).$$

Then, under the linear transformation

$$\left.\begin{aligned} x &= \alpha x' + \beta y' \\ y &= \gamma x' + \delta y' \end{aligned}\right\} \qquad \Delta = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \neq 0, \tag{2}$$

we have the following identity

$$\theta(a_0', a_1', \cdots;\ x', y';\ X, Y) = \Delta^s\theta(a_0, a_1, \cdots;\ x, y;\ X, \Delta^{t+1}Y). \tag{3}$$

This means that the coefficients of the various terms in X and Y in the function θ are covariants of F. In case we take f as the function g, the covariants of f thus obtained he calls the *covariants associated with f.*

If d is the order of the covariant h, then we can write $(1/d)Y$ instead of Y in (1) and (3). If, furthermore, we take as our new variables $xX + x'Y$ and $yX + y'Y$ where $x' = -(1/d)(\partial h/\partial y)$ and $y' = (1/d)(\partial h/\partial x)$, the deter-

[*] "Sur la théorie des fonctions homogènes a deux indéterminées," *Journal für die reine und angewandte Mathematik*, Vol. 52 (1856), pp. 21–23.

minant $xy' - yx'$ of this transformation is the form h itself. The coefficient of X^m will be f itself and the other coefficients will be denoted by h_1, h_2, $\cdots$, h_m; that is,

$$f\left(a_0, a_1, \cdots\ xX - \frac{1}{d}\frac{\partial h}{\partial x} Y,\ yX + \frac{1}{d}\frac{\partial h}{\partial x} Y\right) = f(f,\ h_1,\ h_2,\ \cdots,\ h_m;\ X,\ Y).$$

Thus, if C is any ordinary algebraic covariant of index w, then

$$h^w C\left(a_0, a_1, \cdots;\ xX - \frac{1}{d}\frac{\partial h}{\partial y} Y,\ yX + \frac{1}{d}\frac{\partial h}{\partial x} Y\right) = C(A_0,\ A_1,\ \cdots;\ X,\ Y),$$

where the A_0, A_1, $\cdots$ are respectively f, h_1, $\cdots$, h_m. If we now set $X = 1$ and $Y = 0$, this gives us

$$h^w C(a_0,\ a_1,\ \cdots;\ x,\ y) = C(f,\ h_1,\ \cdots,\ h_m;\ 1,\ 0).$$

Thus he proves his

SECOND PROPOSITION. *Every ordinary algebraic covariant of f, when multiplied by a suitable integral power of h becomes a rational integral function of the associated covariants.*

3. **Extension to Modular Covariants.**—If we now assume that g and h are modular covariants (either formal or otherwise), and follow through Hermite's proof of the First Proposition, we readily see that in this case we obtain the following result,—if g and h are any two modular covariants of f and θ is defined by (1), then when x and y are subjected to the transformation (2) where α, β, γ and δ are marks of the Galois Field $GF[p^n]$ of order p^n, then

$$(4)\quad \theta\left(a_0',\ a_1',\ \cdots;\ x',\ y';\ X,\ \frac{1}{\Delta^{\iota+1}} Y\right) \equiv \Delta^s\theta(a_0,\ a_1,\ \cdots;\ x,\ y;\ X,\ Y).$$

That is,

$$\theta\left(a';\ x',\ y';\ X,\ \frac{1}{\Delta^{\iota+1}} Y\right) = \Delta^s\theta(a;\ x,\ y;\ X,\ Y) + \varphi,$$

where φ vanishes whenever α, β, γ and δ are in the field. Here it must be noted that X and Y are indeterminates. Thus we have

THEOREM I. *The coefficients of the different terms in X and Y are modular covariants (formal or otherwise). If g and h are both formal covariants, then these coefficients are formal covariants; if, however, either g or h is not formally covariant, then the coefficients are not all formal covariants.* In case g is the form f itself, then the covariants obtained in this manner we shall call the *associated covariants of f with respect to the covariant h.*

The above result still holds if we replace $\partial h/\partial x$ and $\partial h/\partial y$ by $\frac{1}{d}\partial h/d\partial x$ and $\frac{1}{d}\partial h/d\partial y$ respectively, where d is the order of h, provided d is not divisible by p. Now for every form f there is always a function h which is covariant under the total group of linear transformations whose coefficients are marks of the field $GF[p]$ and whose order d is not divisible by p.* First, every binary form of odd order > 3 has a (non-vanishing) ordinary algebraic covariant of order one and every binary form of even order > 4 has a covariant of order 2.† Hence we can confine our attention to binary forms of order 3 where $p = 3$ and binary forms of orders 2 and 4 where $p = 2$. Now a binary cubic has an ordinary quadratic covariant.‡ Moreover, the quadratic and quartic modulo 2 have a modular covariant of order one.§ Hence every binary form has with respect to the field $GF[p]$ a modular covariant which is of order $d \neq 0 \pmod{p}$; this is also known to be true with respect to the field $GF[p^n]$ where $n > 1$, provided $p \neq 2$.

Now let C be any modular covariant of f of index w. Without loss of generality, we may assume that C is homogeneous in x and y and pseudo-homogeneous|| in the $a's$, since any covaraint is the sum of a finite number of such covariants. If we replace x and y by $xX + x'Y$ and $yX + y'Y$ respectively, where $xy' - x'y \neq 0$, and x, y, x', y' are indeterminates, then

$$C(A's;\ X,\ Y) \equiv (xy' - x'y)^w C(a's;\ xX + x'Y,\ yX + y'Y)$$

whenever x, y, x', y' are in the field, provided $xy' - x'y \neq 0$. If we now take

$$(6) \qquad x' = -\frac{1}{d}\frac{\partial h}{\partial y} \qquad y' = \frac{1}{d}\frac{\partial h}{\partial x} \qquad (d \neq 0, \text{ mod } p),$$

then the $A's$ become the associated covariants of f with respect to h, and the determinant of the transformation is $h(x, y)$. Hence, on substituting $X = 1$ and $Y = 0$, we find that $C(A's;\ 1,\ 0) \equiv [h(x,\ y)]^w C(a's;\ x,\ y)$ whenever x and y are in the field and $h(x, y) \neq 0$. In case the left member is divisible by $h(x, y)$ and $w > 1$, this congruence is true even when $h(x, y) \equiv 0$; in order to have a congruence which is true without restriction, we multiply throughout by $h(x, y)$ and thus have

$$(7) \qquad h(x,\ y)C(A's;\ 1,\ 0) \equiv [h(x,\ y)]^{w+1} C(a's;\ x,\ y)$$

whenever x and y are in the field.

* Loc. cit., pp. 23–24.

† Clebsch, "Theorie der binäre algebraischen Formen," p. 410; Elliott, "Algebra of Quantics," 1st edition, p. 74.

‡ Gordan, "Invariantentheorie," p. 167; Weber, "Lehrbuch der algebra," Vol. I, p. 223; Elliott, p. 109.

§ Dickson, Madison Colloquium Lectures, p. 56; Glenn, "A System of Formal Covariants, Modulo 2, of the Binary Cubic," *Transactions of the American Mathematical Society*, Vol. 19 (1918), p. 110.

|| We say that a function $\varphi(x, y, \cdots)$ is pseudo-homogeneous of degree d in the Galois Field $GF[p^n]$ of order p^n if $\varphi(\lambda x, \lambda y, \cdots) \equiv \lambda^d \varphi(x, y, \cdots)$ whenever λ is in the field. In case φ is a polynomial, this simply amounts to saying that the degrees of any two terms of φ differ at most by an integral multiple of $p^n - 1$.

First let us consider the case in which C is a non-formal modular covariant. Then, in order to obtain from (7) a congruence which shall be an identity in x and y, we must make (7) homogeneous in x and y. Now the right side is already homogeneous. The order of the left side is determined by the weight of C and the degree of C in the $a's$. But since the weight of any two terms of any modular covariant (such as C) differ at most by integral multiples of $p^n - 1$, it follows that the orders of any two terms B_1 and B_2 of $C(A's;\ 1, 0)$ can differ at most by an integral multiple of $p^n - 1$. Let the degree of B_1 in x and y be ω_1 and let the degree of B_2 be ω_2, where $\omega_1 - \omega_2 = k(p^n - 1)$ and k is a positive integer. Then there is a formal covariant P such that $B_2' = B_2 P^k$ is congruent to B_2 whenever x and y are in the field such that $h(x, y) \not\equiv 0$, and B_2' is of the same degree as B_1 in x and y. We may take $P = Q^\alpha / H^\beta$ where Q is the universal covariant $(x^{p^{n^2}}y - xy^{p^{n^2}})/L$, $H = [h(x, y)]^{p^n - 1}$, and α and β are two positive integers such that $\alpha p^n - \beta d = 1$. Thus, by multiplying each term of the left member of (7) by a suitably high power of P, we can make the left member homogeneous in x and y of a degree greater than that of the right side. Then, if we multiply the right side of (7) by a suitable power of $P' = H^{\beta'}/Q^{\alpha'}$ where α', β' is a pair of positive integers such that $\beta' d - \alpha' p^n = 1$, we can make the right side of (7) of the same degree as the left side.† Thus, by multiplying both sides of the congruence just obtained by a suitable power of P', we obtain from (7) a congruence which is equivalent to (7) whenever x and y are in the field. This congruence we may write

$$(8) \qquad [h(x, y)]^r C(a;\ x, y) \equiv \mathfrak{C}(Q, h, A's).$$

Since this is homogeneous in x and y and holds for all values of x and y in the field, we have the identity

$$(9) \qquad [h(x, y)]^r C(a;\ x, y) \equiv \mathfrak{C}(Q, h, A's) + LC_1$$

where C_1 is a modular covariant and $\mathfrak{C}$ is a polynomial in its arguments.

Hence we have proved

THEOREM II. *Let $f(x, y)$ be any modular form with coefficients $a_0, a_1, \cdots,$ in the Galois field $GF[p^n]$ of order p^n, and let $h(x, y)$ be any modular covariant of $f(x, y)$—whose order $\not\equiv 0$—under any group G of linear transformations with coefficients in the field. If $C(a's;\ x, y)$ is any modular covariant of $f(x, y)$, then—aside from a power of h—$C(s's;\ x, y)$ is equal to a polynomial in Q and the associated covariants of f with respect to h plus L times a modular covariant. Observe that, unless $p = 2$, there is always an ordinary algebraic*

[*] Dickson, "Invariants of Binary Forms under Modular Transformations," *Transactions of the American Mathematical Society*, Vol. 8 (1907), p. 209.

[†] Note that we can take α and β such that $\alpha < d$ and $\beta < p^n$. With this choice of α and β, we can take $\alpha' = -\alpha + d$, $\beta' = -\beta + p^n$.

covariant satisfying the above conditions for h; and hence, unless $p = 2$, the associated covariants of f with respect to h are all ordinary algebraic covariants of f.

4. Several Corollaries.—If, in Theorem II, we take $h = f$ and $x = 1$, $y = 0$, we have

COROLLARY I. *Aside from a power of a_0, every modular seminvariant of a binary form f whose order is not divisible by p is a polynomial in the ordinary seminvariants of f.*

Observe that this is not equivalent to saying that, aside from a power of a_0, every modular seminvariant of f is an ordinary seminvariant of f; for, in order that a polynomial in ordinary seminvariants be an ordinary seminvariant, it must be homogeneous in the a's and isobaric, whereas, a modular seminvariant is not necessarily either homogeneous or isobaric.

We can also derive a method of constructing a modular covariant having a given seminvariant as leader. For, if $C(a's;\ x, y)$ is any function having the invariantive property under a transformation T, then equation (5) holds provided x and y have such values that

$$\bar{x} = xX - \frac{1}{d}\frac{\partial h}{\partial y}Y, \qquad \bar{y} = yX + \frac{1}{d}\frac{\partial h}{\partial x}Y,$$

is the transformation T. In case C is a seminvariant, (5) must be true whenever $y = 0$ and x is in the field. Thus for a seminvariant, (7) and (8) hold when $y = 0$ and x is in the field. Since equation (8) is homogeneous in x and y, this means that the leader of $\mathfrak{C}$ is C times the r'th power of the leader of h. In case the leader of h is a factor of the seminvariant C, then the leader of $h^{p^n-r-1}\mathfrak{C}$ is C. In case the order of the form f is not divisible by p, we may take $h = f$, and thus we prove the following

COROLLARY II. *Let $f(x, y)$ be a binary form of order $m \not\equiv 0$ (mod p), and let $S(a_0, a_1, \cdots)$ be any modular seminvariant of f with respect to the Galois field $GF[p^n]$ of order p^n. If S contains a_0 as a factor, then a modular covariant having the given seminvariant as leader is obtained by making $S(A_0, A_1, \cdots)$ homogeneous in x and y by the method used in § 3 and then multiplying by a suitable power of a_0. Here $A_0, A_1, \cdots$ are the ordinary algebraic covariants which Hermite called the associated covariants of f.*

5. Theorem for Formal Covariants.—In case $C(a's;\ x, y)$ is a formal modular covariant of a binary form $f(x, y)$, we have

$$h(x, y)C(A's;\ 1, 0) \equiv [h(x, y)]^{w+1}C(a's;\ x, y) \tag{7}$$

holding whenever x, y and the a's are all in the field. Since C is a formal covariant, we may without loss of generality assume that C is homogeneous in x and y and homogeneous in the a's. Then the left member of (7) is pseudo-homogeneous in x and y and pseudo-homogeneous in the a's. We now have the double task of making (7) homogeneous in the a's as well as homogeneous in x and y. To do this, first make (7) homogeneous in x and y by multiplying each term by a suitable power of P, just as in § 3. Thus we have

$$(9) \qquad [h(x, y)]^r C(a;\ x, y) \equiv \mathfrak{C}(Q, h, A's) + LC_1,$$

holding whenever the a's are marks of the field. Now any two terms of (9) are of the same order, but of different degrees in the a's, their degrees differing at most by an integral multiple of $p^n - 1$. Let the difference between the lowest degree and the highest degrees be $k(p^n - 1)$. Then multiply (9) throughout by $[h(x, y)]^k$. If $h'(x, y)$ denote the polynomial obtained from $h(x, y)$ by replacing $a_0, a_1, \cdots$ by $a_0^{p^n}, a_1^{p^n}, \cdots$, then $h'(x, y) \equiv h(x, y)$ when the a's are marks of the field. Moreover $h'(x, y)$ is a formal covariant.* Hence we may replace h in (9) wherever we wish by h' without changing the validity of the congruence or the formal covariancy. If, in any term we replace h^l by h'^l where the degree of that term is $l(p^n - 1)$ less than the maximum degree of any such term, we obtain a congruence which we may write

$$(10) \quad [h(x, y)]^q\, [h'(x, y)]^{r-q} C(a;\ x, y) \equiv \mathfrak{C}'(Q, h, h', A's) + LC_1' + K$$

where K is a formal covariant (since all the other functions in the congruence are formal covariants) which is congruent to zero whenever the a's are in the field. Thus once more we see the importance of those irreducible formal covariants which are congruent to zero for all values of the coefficients in the field.† Thus we have proved

THEOREM III. *Let $f(x, y)$ be any form with coefficients $a_0, a_1, \cdots$ which are indeterminates, and let $h(x, y)$ be any formal covariant of $f(x, y)$ under a group of linear transformations having coefficients in the Galois field $GF[p^n]$ of order p^n. Moreover, let the order of $h(x, y)$ be not divisible by p. If $C(a's;\ x, y)$ is any formal covariant of $f(x, y)$, then if we multiply $C(a's;\ x, y)$ by a suitable power of $h(a's;\ x, y)$ and by a suitable power of $h(a^{p^n};\ x, y)$ the result is identically congruent to a polynomial in Q, L and the irreducible formal covariants which vanish whenever the a's are in the field. The coefficients of the different powers of Q are polynomials in $h(a's;\ x, y)$, $h(a^{p^n};\ x, y)$ and the formal covariants which are the associated covariants of $f(x, y)$ with respect to $h(x, y)$.* Notice that, unless $p = 2$, the covariant $h(x, y)$ can be taken as an ordinary algebraic covariant.

* O. E. Glenn, "Modular Invariant Processes," *Bulletin of the American Mathematical Society*, Vol. 21 (1915), pp. 167–173.

† In a recent paper (*Transactions of the American Mathematical Society*, Vol. 22 (1921), April issue) the writer proved that the set of all formal covariants of a system of forms S has the finiteness property if and only if the finiteness property is possessed by the set of those formal covariants of S which vanish whenever the coefficients of S are marks of the field.

6. Verification for the Binary Quadratic, Modulo 3.—Dickson[*] has shown that a fundamental set of modular covariants of the binary quadratic, $f_2 = a_0x_1^2 + 2a_1xy + a_2y^2$ (mod 3) consists of

$$f_2, \qquad f_4 = a_0x^4 + a_1x^3y + a_1xy^3 + a_2y^4,$$

$$L = x^3y - xy^3, \qquad Q = x^6 + x^4y^2 + x^2y^4 + y^6,$$

$$\Delta = a_1^2 - a_0a_2, \qquad q = (a_0 + a_2)(a_1^2 + a_0a_2 - 1),$$

$$C_1 = (a_0^2a_1 - a_1^3)x^2 + 2(a_1^2 + a_0a_2)(a_2 - a_0)xy + (a_1^3 - a_1a_2^2)y^2,$$

$$C_2 = (\Delta + a_0^2)x^2 - 2a_1(a_0 + a_2)xy + (\Delta + a_2^2)y^2.$$

By Hermite's fundamental memoir, the associated covariants of f_2 are $A_0 = f_2$, $A_1 = 0$, $A_2 = -\Delta f_2$. Theorem II is clearly true for polynomials in f_2 and Δ, since these are ordinary algebraic covariants.

If we take $C = f_4$, then since here $C(A's;\ 1,\ 0) = A_0 = f_2$, (7) becomes $f_2 \equiv f_4$ (whenever x and y are in the field) and (8) becomes $f_2^3f_4 \equiv f_2^2Q - L^2C_2$. When $C = C_1$, we find that (8) becomes[†] $0 \equiv f_2C_1 + (\Delta^2 + \Delta)L$. For $C = C_2$, (8) becomes $(1 + \Delta)f_2^2Q \equiv f_2^4C_2 + L^2(qf_2 - C_2)$. Thus the theorem is verified when C is any polynomial in Δ, f_2, f_4, C_1, C_2 and L, Q. Is it true for any covariant containing q as a factor, say qQf_2? For $C = qQf_2$, $C(A's;\ 1,\ 0) = (f_2 + \Delta f_2)(\Delta f_2^2 - 1)f_2Q \equiv (\Delta^2 - 1)f_2^4$ when x and y are in the field, and thus we have $qQf_2 \equiv (\Delta^2 - 1)f_2^4 - q^2L^2$.

7. Relation to the Literature.—The chief interest of the results of this paper lies in the relation shown to exist between modular covariants and ordinary algebraic covariants of the form. From a different point of view, the results are of interest in connection with several papers by Professor Glenn.

He considered the expansion of a homogeneous binary form in terms of two binary forms of lower order.[‡] He found that a binary form f of order $n(m + 1) - 1$ can be expressed in the form

$$f = \varphi_{0p}f_{1n}^m + \varphi_{1p}f_{1n}^{m-1}f_{2n} + \cdots + \varphi_{mp}f_{2n}^m$$

(where f_{1n} and f_{2n} are two binary forms of orders n and the φ's are binary forms of order p) provided the resultant R of f_{1n} and f_{2n} does not vanish. Moreover this expansion is unique for any such pair of forms f_{1n}, f_{2n}.

[*] *Transactions of the American Mathematical Society*, Vol. 14 (1913), p. 310.

[†] This syzygy was given by Dickson, "Finiteness of Modular Covariants," *Transactions of the American Mathematical Society*, Vol. 14 (1913), p. 310.

[‡] "The Symbolical Theory of Finite Expansions," *Transactions of the American Mathematical Society*, Vol. 15 (1914), pp. 72–86.

He also showed that a form f of order m can be expressed linearly in terms of two forms f_{1n_1} and f_{2n_2} of different orders n_1 and n_2 respectively, provided the resultant of f_{1n_1} and f_{2n_2} is different from zero.* Thus

$$f_m = \varphi_{1m-n_1}f_{1n_1} + \varphi_{2m-n_2}f_{2n_2} \tag{11}$$

where φ_{1m-n_1} and φ_{2m-n_2} are of orders $m - n_1$ and $m - n_2$ respectively. If $n_1 + n_2 = m + 1$, the expansion is unique.

If f_{1n_1} and f_{2n_2} are covariants of f and the expansion is unique, then the forms φ_{1m-n_1} and φ_{2m-n_2} are covariants of f. If, furthermore, (11) is a congruence modulo p a prime, and $f_{1n_1} = Q$, $f_{2n_2} = L$ where

$$L = x^py - xy^p, \qquad Q = (x^{p^2}y - xy^{p^2}) \div L = x^{p(p-1)} + \cdots + y^{p(p-1)},$$

then we have

$$f_m \equiv Q\varphi_1 + L\varphi_2 \pmod{p} \tag{12}$$

and it appears that any binary form of order $m = p^2$ is reducible in terms of Q and L and two first degree formal modular covariants with respect to the $GF[p]$ whose orders are respectively p and $p^2 - p - 1$.† As Professor Glenn points out, "this raises the question as to whether the modular expansions (12) for $m > p^2$, containing arbitrary parameters in their coefficients may have these parameters determined so that the coefficient forms φ_{1m-p^2+p}, φ_{2m-p-1} are modular covariants." For various cases in which $m > p^2$, he has determined modular covariants φ_1 and φ_2 of f such that the congruence (12) will hold identically in the a's and the variables x, y.

Theorem II of the present paper shows that, for any Galois Field $GF[p^n]$ of order p^n, if a modular covariant C of f be multiplied by a sufficiently high power of h, then it is expressible in the form $Q\varphi_1 + L\varphi_2$ where φ_1 and φ_2 are modular covariants of f. Moreover, φ_1 is a polynomial in Q, f, h and the associated covariants of f with respect to h. At present I do not know whether it is true that, for every covariant of f, there is one such expansion in which φ_2 is of lower order than C. If this be so, then it would follow by induction that, aside from a power of h, every modular covariant of f is a polynomial in Q, L, f, h and the associated covariants of f with respect to h.

MOUNT HOLYOKE COLLEGE,
SOUTH HADLEY, MASS.

* "A Memoir on the Doctrine of Associated Forms," *Transactions of the American Mathematical Society*, Vol. 18 (1917), pp. 443–462 (especially pp. 446–448).

† See article referred to in previous note, p. 461.